NSTIC Pre-Plenary Event 3/15

Consumer/Civil Liberty and Privacy Protections

Synopsis
Summary: The group discussed privacy concerns and suggested methods to enhance privacy for individuals participating in the identity ecosystem. The group first explored different business models for entities participating in the identity ecosystem. The group found many opportunities for organizations to augment existing services to consumers, but stressed that these organizations must be able to demonstrate the value of these services to consumers. The group thoroughly discussed commercial data usage and concluded that preventing nefarious use of data is important. The group also discussed the role of the Privacy Coordination Committee in the Steering Committee, proactively engagement with working groups to ensure that they build privacy into their proposals, and the role of the gatekeeping function in driving early engagement and "privacy by design." Finally, the group discussed the trustmark that the NSTIC will create and the role of auditing and the ability to revoke the trustmark as best methods to enforce the underlying rules of the trustmark. The breakout session took the format of open dialogue/discussion. There were no slides.

Discussion Points/Decisions		
No.	**Topic**	**Discussion/Decisions**
1.	Business Models	The group discussed the tension between individual privacy needs and business data consumption models.
		The group discussed whether individuals would pay higher upfront costs for credentials. The group agreed that individuals would more likely choose solutions that use a transaction-based cost structure.
		The group discussed a case involving Japan Airlines. Japan Airlines used identities to direct individuals to hotels, car rentals, and other businesses that partnered with them. Individuals could then easily buy services from those partners using their Japan Airlines identity in "frictionless" transactions. The main issue in expanding the service is that potential partners see privacy risks associated with the transactions.
		The group discussed transactions where an organization might not know a person's name, but his or her behaviors (i.e. using a loyalty card).
		The group discussed a model based on the credit card industry where relying parties pay for part of the transaction. One group member stated that the business model for credentials differed from this model because the identity ecosystem will save relying parties money.
		The group debated the idea that existing organizations could offer additional services such as identity proofing. Some group members did not like the idea of public sector entities offering these services. Others saw value in locking customers by offering easily repeatable transactions. The group mentioned that an organization must be ubiquitous to offer identity proofing services because people will not trust organizations they do not know.

Discussion Points/Decisions	
2. Gatekeeper Function	The group agreed that the Privacy Coordination Committee must engage working groups early on in proposal development to address privacy issues. The group mentioned that privacy should develop and distribute evaluation criteria to working groups to ensure that they build privacy into their proposals.
	The group discussed how the gatekeeping function might lead to the perception of the Privacy Coordination Committee as a roadblock. The group observed that the Committee cannot reject all proposals because these actions would lead to that perception. Ultimately, there was recognition that the gatekeeping function could be used to drive the working groups to early engagement with privacy experts to avoid a roadblock outcome at the end of the process.
	The group suggested using proposal rejection rate as a metric to determine the success of the Privacy Coordination Committee. The group suggested that high levels of rejection would indicate that the Committee needed to reevaluate its processes.
	The group discussed whether evaluation of proposals by the Privacy Steering Committee was binary. The group discussed issues involved in sending proposals to the plenary that did not adhere to established privacy criteria.
3. Privacy Discussion	The group discussed individual ownership of the data. The group also discussed the ability of an individual to transfer data if an individual discontinues business with a company. One group member suggested that NSTIC focus on individual control over data. Other group members stated that organizations don't want to allow individuals to have control over data.
	The group discussed whether companies must de-identify data prior to sharing it. The group noted that cryptographic technology exists that allows organizations to de-identify data.
	The group discussed the importance of reputation to high assurance identity providers. The group suggested that lower assurance identity providers might follow high assurance organizations if the high assurance organizations subscribe to NSTIC privacy rules.
	The group indicated that all organizations use data, but this differs from data abuse. The group suggested that disabling nefarious usage of data is important. Some group members suggested the NSTIC should not allow large data transfers and data linking practices.
	The group discussed the challenge of implementing a privacy framework that covers both low and high level of assurance identity providers. The group observed that many organizations that offer high level assurance are already regulated.
	The group discussed whether the NSTIC could address privacy issues that exist outside the identity ecosystem.
4. Trustmark	The group discussed a privacy trustmark developed in Japan. The government originally administered the trustmark, but eventually transferred those duties to the private sector.
	Some group members proposed the creation of multiple trustmarks, each with different levels of privacy and accreditation.
	The group stressed the importance of auditing to ensure that organizations using the trustmark adhere to privacy rules. The group advised that the NSTIC must be prepared to revoke trustmarks in cases where an organization does not

Discussion Points / Decisions	
	adhere to the underlying rules. The group agreed that the Steering Committee must carry insurance to limit liability in cases where an organization carries its trustmark and does not adhere to the rules.
5. Value to Individuals	The group discussed how the ease of use traits of credentials in the identity ecosystem would lead individuals to use them.
	The group discussed a model where using credentials in the identity ecosystem would reduce fraud and identity theft. The group suggested that businesses could inform consumers that using one of these credentials could reduce their liability should they become a victim of fraud or identity theft.